Testimony of Frederick (Ted) Peters to the House Subcommittee on Homeland Security on Cybersecurity

April 16, 2014

Thank you for having me as a witness in this area of critical importance to our country. As a banker for almost forty years, I will try to focus my comments and testimony on issues relating to the financial services industry and its clients.

Some quick background information on the Bryn Mawr Trust Company, where I currently serve as Chairman and CEO. At Bryn Mawr Trust we recently celebrated our 125th anniversary as a Philadelphia area financial institution. We are a $9.5 billion organization, with over $2 billion of banking assets and $7.5 billion of trust and investment assets under management or administration in the states of Pennsylvania and Delaware. We serve primarily individuals and closely-held businesses which operate in this region. Not only have we survived numerous wars, recessions, and depressions, but have thrived and are one of the highest-performing banks in the nation.

All banks and financial institutions are extremely alarmed at the actual and potential threats of Cyber crime. At our bank we have devoted extraordinary amounts of time, man and woman power, and money to protect our Bank and all of our clients from this growing problem.

In the United States and world-wide, Cyber crime and Cyber threats are multiplying at an alarming rate. These threats come in the form of hacking, phishing, its more sophisticated derivative spear-fishing, malware intrusion, and the well-publicized DDoS or "Distributed Denial of Service" attacks on larger U.S. financial institutions.

Who are the "bad guys" ?

They are no longer precocious teenagers operating at 3 in the morning in their parents' rec rooms. Today's perpetrators are high-level professionals and fall into a number of categories.

Organized crimes-rings are responsible for over half of all attacks. These are well-organized groups which operate in a structured and efficient manner with profit and loss statements much like a legitimate business. Their sophistication is extremely high and improving almost daily.

Next are state-supported enterprises which comprise about a quarter of all attacks. These enterprises have different motives than organized crime and are usually looking for intelligence information that would give a nation-state some political or military advantage. Primary offenders here are China and former satellite countries of the Soviet Union such as Bulgaria, Romania, and the Ukraine

A third group would be the "hacktivists" and you have probably heard of some of these groups such as "Anonymous" or the "Tunsian Hackers Team". These organizations are usually not seeking financial gain, but are more interested in making headlines. Although "hacktivists" only account for a small % of attacks, they have been very successful in creating a series of high-profile DDoS against financial institutions in the United States.

And lastly, current and former employees and vendors also provide a serious threat. I think we have all heard of a gentleman named Edward Snowden.

One of the biggest threats to banks around the country are "corporate and individual account takeovers" initiated by malware being secretly installed on a business or person's computer. Again you will recognize some of the names of this malware - Citadel, Trojan, and Zeus. Once inside, the perpetrator will then move money around and eventually try to clean out the accounts.

"Point of Sale" payment systems are another target of malware criminals. Once the malware is secretly installed on a merchant's computer, the malware allows cyber-criminals to access all of the unencrypted credit card and debit card information, and at times the encrypted data as well.

What is the solution ? Unfortunately there is no 100% solution. The cyber-criminals are out there always trying to stay one step ahead of the "good guys". The following, however, are considered "best practices;" to reduce the possibility of any attack being successful.

First, businesses and individuals need to use a multi-layered approach. This means a combination of many risk-based, predictive, and behavioral technologies which are out there. Companies and consumers who provide a "hardened target" will find the cyber-criminal moving on to a new and easier possible victim.

Next, build a strong "feedback loop" so that any intrusion can be identified and defended accordingly.

And lastly, continue to perform on-going assessments of risk and improving one's defenses.

With that, Mr Chairman, my testimony is concluded.